Amendments to the claims:

This listing of claims will replace all prior versions and listings of claims in the application:

Listing of claims:

1. (Currently Amended) A network system for determining trivial keyboard sequences of a proposed password, comprising:

a user system;

a computer keyboard input device associated with said user system;

a server in communication with said user systems via a communications link;

a data storage device coupled to said server, said data storage device housing:

a database including a keyboard profile wherein said keyboard profile specifies a physical layout of character and function keys on said computer keyboard input device;

a master password database including a user account associated with said user system; and

a password verification mechanism executable by said server;

wherein, upon execution, said password verification mechanism performs an algorithm on said proposed password and determines triviality of said proposed password according to criteria specified in said algorithm.

2-5. (Canceled)

6. (Original) The network system of claim 1, wherein said algorithm comprises three formulas wherein:

a first formula checks for vertical triviality of said proposed password;

a second formula checks for horizontal triviality of said proposed password; and

a third formula checks for diverse keystroke patterns of said proposed password;

wherein said second formula is executed upon successful validation of said first formula; and said third formula is executed upon successful validation of said second formula.

7. (Original) The network system of claim 6, wherein successful validations of any of said three formulas causes said password verification mechanism to:

transmit notification to at least one of:

a requesting user system; and

an administrator system; and

update said master password database.

8-10. (Canceled)

11. (Currently Amended) A method for determining keyboard triviality of proposed passwords over a network system, comprising:

receiving a request for a proposed password from a user system;

retrieving user account data related to said user system;

checking said proposed password against existing password quality rules stored in a master password database, wherein a requester of said proposed password is redirected to select an alternative password if said checking results in an unacceptable password;

providing a keyboard profile associated with said user system, said keyboard profile including a unique identifier;

performing an algorithm on said proposed password, said algorithm including a first formula, comprising:

$(\Delta X1 + \Delta X2 + \ldots + \Delta X_{(n-1)})/(n - 1) > 0;$

wherein:

X represents data coordinate of each character of said proposed password on an X axis of the keyboard profile;

~~Y represents an Y axis;~~

n represents a number of the characters comprising said proposed password; and

$\Delta X1$ represents an absolute value of a difference between a first and second data coordinate on said X axis;

and wherein further data coordinates are plugged into said first formula for determining vertical triviality.

12. (Currently Amended) The method of claim 11, wherein said algorithm includes a second formula executable upon successful completion of said first formula, comprising:

$(\Delta Y1 + \Delta Y2 + \ldots \Delta Y_{(n-1)})/(n - 1) > 0;$

wherein:

~~X represents an X axis;~~

Y represents data coordinate of each character of said proposed password on a Y axis of the keyboard profile;

n represents a number of the characters comprising said proposed password; and

$\Delta Y1$ represents an absolute value of a difference between a first and second data coordinate on said Y axis;

and wherein further data coordinates are plugged into said second formula for determining horizontal triviality.

13. (Currently Amended) The method of claim 11, wherein said algorithm includes a third formula, comprising:

$(\Delta X1 + \Delta Y1 + \Delta X2 + \Delta Y2 + \ldots + \Delta X_{(n-1)} + \Delta Y_{(n-1)})/(2(n - 1)) >= S;$

wherein:

X represents data coordinate of each character of said proposed password on an X axis of the keyboard profile;

Y represents data coordinate of each character of said proposed password on a Y axis of the keyboard profile;

n represents a number of the characters comprising said proposed password;

ΔX1 represents an absolute value of a difference between a first and second data coordinate on said X axis;

ΔY1 represents an absolute value of a difference between a first and second data coordinate on said Y axis; and

S represents a variable parameter representing a mean distance between character keys of proposed passwords;

and wherein further data coordinates are plugged into said third formula for determining diverse keystroke patterns of said proposed password.

14. (Original) The method of claim 13, wherein successful completion of said algorithm causes a password verification mechanism to:

transmit acceptance of said proposed password to at least one of:

said user system;

an administrator system; and

update a password database to reflect said acceptance.

15. (Original) The method of claim 11, wherein said identifier is linked to said user account, and wherein further, said keyboard profile is automatically provided over said network system via said link.

16. (Original) The method of claim 11, wherein a list of available keyboard profiles are presented to said user selection, and wherein further, said user system selects an appropriate profile.

17. (Currently Amended) A storage medium encoded with machine-readable computer program code for determining keyboard triviality of proposed passwords over a

network system, the storage medium including instructions for causing said computer network to implement a method comprising:

receiving a request for a proposed password from a user system;

retrieving user account data related to said user system;

checking said proposed password against existing password quality rules stored in a master password database, wherein a requester of said proposed password is redirected to select an alternative password if said checking results in an unacceptable password;

providing a keyboard profile associated with said user system, said keyboard profile including a unique identifier;

performing an algorithm on said proposed password, said algorithm including a first formula, comprising:

$(\Delta X1 + \Delta X2 + ... + \Delta X_{(n-1)})/(n - 1) > 0;$

wherein:

X represents data coordinate of each character of said proposed password on an X axis of the keyboard profile;

~~Y represents a Y axis~~;

n represents a number of the characters comprising said proposed password; and

$\Delta X1$ represents an absolute value of a difference between a first and second data coordinate on said X axis;

and wherein further data coordinates are plugged into said first formula for determining vertical triviality.

18. (Currently Amended) The storage medium of claim 17, wherein said algorithm includes a second formula executable upon successful completion of said first formula, comprising:

$(\Delta Y1 + \Delta Y2 + ... \Delta Y_{(n-1)})/(n - 1) > 0;$

wherein:

X represents said X-axis;

Y represents data coordinate of each character of said proposed password on said Y axis;

n represents a number of the characters comprising said proposed password; and

$\Delta Y1$ represents an absolute value of a difference between a first and second data coordinate on said Y axis;

and wherein further data coordinates are plugged into said second formula for determining horizontal triviality.

19. (Currently Amended) The storage medium of claim 17, wherein said algorithm includes a third formula, comprising:

$(\Delta X1 + \Delta Y1 + \Delta X2 + \Delta Y2 + ... + \Delta X_{(n-1)} + \Delta Y_{(n-1)})/(2(n - 1)) >= S;$

wherein:

X represents said x-axis;

Y represents data coordinate of each character of said proposed password on said y axis;

n represents a number of characters comprising said proposed password;

$\Delta X1$ represents an absolute value of a difference between a first and second data coordinate on said X axis;

$\Delta Y1$ represents an absolute value of a difference between a first and second data coordinate on said Y axis; and

S represents a variable parameter representing a mean distance between character keys of proposed passwords;

and wherein further data coordinates are plugged into said third formula for determining diverse keystroke patterns of said proposed password.

20. (Original) The storage medium of claim 19, wherein successful completion of said algorithm causes a password verification mechanism to:

transmit acceptance of said proposed password to at least one of:

said user system;

an administrator system; and

update a password database to reflect said acceptance.

21. (Original) The storage medium of claim 17, wherein said identifier is linked to said user account, and wherein further, said keyboard profile is automatically provided over said network system via said link.

22. (Original) The storage medium of claim 17, wherein a list of available keyboard profiles are presented to said user selection, and wherein further, said user system selects an appropriate profile.